Assuring Critical Government Services: Treasury's Perspective

Presented by

Ray E. LaVan, Jr.

Director, Office of Security and Critical Infrastructure Protection

U.S. Department of the Treasury

JUNE 27, 2000

Our Agenda

- Treasury Missions
- Nature and Scope of the CIP Challenge
- Strategic CIP Planning Considerations
- Treasury's Response to PDD-63
- Treasury CIP/Security Initiatives
- Looking Ahead

Treasury Mission

- Promote prosperous and stable American and world economy
- Manage the U.S. Government’s finances
- Protect our financial institutions and our nation’s leaders
- Continue to build and maintain a strong institution to accomplish the above

Nature and Scope of the Challenge

- We are vulnerable
- There are lots of threats: from traditional and cyber-criminals, to terrorists, to avowed national enemies , to unhappy employees and disgruntled opportunists
- A single computer virus can cause as much monetary damage as Hurricane Andrew, or worse
- Economic and national security are increasingly interrelated and co-exist in a symbiotic relationship

Nature and Scope of the Challenge

- Security is no longer something extra. It ***must*** be an integral part of the way we do business.
- Everyone ***must*** play a role in security
- Government and industry ***must*** increasingly work together to achieve mutual security objectives through collaboration, cooperation, partnership, integration and mutually developed technological protections to traditional and emerging threats

Nature and Scope of the Challenge

- How to protect 150,000 employees in 22,000 offices located in 1800 facilities and hundreds of cyber systems
- Which of these, if lost, would ***most significantly impact*** US national and economic security and essential Treasury functions
- How can we improve

Strategic Planning Considerations

- CIP is ***NOT*** simply “cyber”, but the purposeful integration of six security-oriented disciplines:
  - ***Information Systems Security***
  - ***Physical Security***
  - ***Personnel Security***
  - ***Information Security***
  - ***Industrial Security***
  - ***Emergency Preparedness***

Strategic Planning Considerations

- The programs required to protect and assure cyber systems would have to be built in the years ahead
- The traditional security disciplines would have to define their role to protect and assure “critical assets” as opposed to all assets

Treasury's Response to PDD-63

- Treasury Critical Infrastructure Protection Plan (TCIPP)
- Treasury Infrastructure Protection Panel (TIPP) chaired by the Treasury CIAO and CIO
- CIO Cyber CIP Working Group formed at HQ-level to coordinate cyber efforts
- Critical Infrastructure Protection Officer at HQ-level to lead non-cyber and multi-disciplinary integration efforts

FY2000 CIP Program Initiatives

- Cyber Focus (<$1million):
  - identifying critical systems
  - providing key profile data to support vulnerability assessments
  - assessing intrusion detection tools
  - development of a cyber intrusion detection and response capability
- Non-Cyber Focus (<$1million):
  - identifying critical facilities
  - physical security review
  - CIP integration across the Department

Security programs support CIP

- We conduct background investigations of employees and contractors working in critical facilities or on critical systems
- We protect classified and sensitive information, the loss of which, could adversely impact Treasury Critical Infrastructure (TCI)
- Physical security programs protect our facilities against various threats
- Emergency preparedness planning provides CIP assurance

New Initiatives

- Insider Threat Working Group
- INPROTECT 2000
- Facility Security Profile Management
- Investments in Training

Looking Ahead

- The overall outlook for CIP is bright ***if:***
  - an integrated, ***multi-disciplinary*** CIP philosophy and program approach is used
  - we establish the right relationships
  - timely threat/event identification, preparedness, mitigation, response and recovery mechanisms are established, understood ***and routinely exercised***
  - we invest in research and technology
  - we provide tailored training, education and awareness programs

For More Information on Treasury’s Critical Infrastructure Protection Program Contact:

Ray E. LaVan, Director
Office of Security and Critical Infrastructure Protection
Department of the Treasury
Tel: (202)-622-1120
ray.lavan@do.treas.gov

or

Ronald Bearse
Critical Infrastructure Protection Officer
Tel: (202)-622-2059
ron.bearse@do.treas.gov